IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2136
Christopher E. Barnabo et al.	:	Examiner: David Garcia Cervetti
Serial No.: 10/600,215	:	IBM Corporation
Filed: 06/20/2003	:	Intellectual Property Law
Title: SYSTEM AND METHOD FOR AUTHENTICATION TO AN APPLICATION	:	Department SHCB/040-3
	:	1701 North Street
	:	Endicott, NY 13760
Confirmation No.: 5835		

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Corrected Section V. for Appeal Brief

V. Summary of Claimed Subject Matter

Support for the claim elements is indicated in plain brackets [ ].

Claims 1, 16 and 21 recite a method, system and program product for authenticating a first user [user 25 of Figure 1] in a protected network [Blue Zone network 12] to an application [Application 30 of Figure 1 and Page 5 lines 8-13 and 16-21] shared concurrently with a second user [User 53 in Figure 1 in Red Zone network 16. Page 8 lines 25-26] in an unprotected network. [Red Zone network 16 or Internet 54] The first user [User 25 in Blue Zone 12] supplies a userID and a password to a first server [Server 20] within the protected network for authentication for the application. [Steps 100-105 of Figure 3A and Page 6 line 22 to Page 7 line 4.] The application [Application 30] resides in a third network [Yellow Zone network 14] configured as a buffer between the protected network [Blue Zone network 12] and the unprotected network [Red Zone network 16]. The user's password is not sent from the protected network into the third network to access the application. [Page 7 lines 9-18.] The first server determines that the userID and password are authentic. [Step 104 and Decision 105, yes branch

and Page 7 lines 1-4.] In response, the first server [Server 20] forwards to the application [Application 30] an authentication key for the first user and a selection by the first user pertaining to the application. [Step 110 and Page 7 lines 9-26.] The application determines that the key is authentic. [Step 114 and 116 and Page 7 line 26 to Page 8 line 4.] In response, the application complies with the selection by the first user. [Step 124 and Page 8 lines 3-7.] The second user [User 53 in Red zone] supplies another userID and another password to the application. [Steps 300, 302 and 304 of Figure 4A and Page 8 line 25 to Page 9 line 1.] The application determines that the other userID [for User 53 in Red Zone] and the other password are authentic [Step 306 and Decision 308, yes branch and Page 9 lines 1-4], and in response, the application complies with a selection made by the second user pertaining to the application. [Step 316 and Page 9 lines 3-5.]

Claim 14 depends on claim 1 and recites that the authentication key is self authenticating based on whether a period during which the key is valid matches a scheduled period of use of the application, and whether an IP address of the first user is from the protected network [Page 7 line 23 to Page 8 line 1.]

Independent claim 23 recites a method for authenticating a first user [user 25 of Figure 1] of a first computer [Computer 24 of Figure 1] in a protected network [Blue Zone network 12] to a second computer [Computer 40] executing an application [Application 30 of Figure 1 and Page 5 lines 8-13 and 16-21]. A second user [User 53 in Figure 1 in Red Zone network 16. Page 8 lines 25-26] of a third computer [Computer 52] in an unprotected network [Red Zone network 16 or Internet 54] and the first user of the first computer concurrently share the application [Application 30]. The second computer [Computer 40] resides in a third network [Yellow Zone network 14] configured as a buffer between the protected network [Blue zone network 12] and the unprotected network [Red zone network 16]. The first computer supplies a userID and a password of the first user to a fourth computer [Server 20] in the protected network for authentication for the application [Application 30]. The fourth computer [Server 20] determines that the userID and password are authentic [Step 104 and Decision 105, yes branch of Figure 3(a) and Page 7 lines 1-4]. In response, the fourth computer forwards to the second computer an authentication key for the first user [Step 110 of Figure 3(b) and Page 7 lines 9-26]. The

password is not sent from the protected network into the third network to access the application [Page 7 lines 9-18]. The second computer determines that the key is authentic [Step 114 and Decision 116, yes branch of Figure 3(b) and Page 7 line 26 to Page 8 line 4], and in response, complies with a selection by the first user pertaining to the application [Step 124 of Figure 3(c) and Page 8 lines 3-7]. The third computer supplies another userID and another password of the second user to the second computer [Steps 300, 302 and 304 of Figure 4A and Page 8 line 25 to Page 9 line 1]. The second computer determines that the other userID [for User 53 in Red Zone] and the other password are authentic [Step 306 and Decision 308, yes branch of Figure 4(a) and Page 9 lines 1-4]. In response, the application complies with a selection made by the second user pertaining to the application [Step 316 of Figure 4(a) and Page 9 lines 3-5].

Structure, material or acts corresponding to each means plus function element are indicated in stylized brackets { }.

16. An authentication system comprising:

an application [Application 30, Page 5 lines 8-13 and 16-21, and equivalents] on a first server [Server 40, and equivalents] in a first network [Yellow Zone or buffer network 14, and equivalents];

a second server {Server 20 and equivalents} in a second, protected network {Blue Zone 12 or Intranet 22 and equivalents and equivalents} to receive from a first user {user 25, and equivalents} within said second network a userID and a password for authentication for said application, said second server including means for checking authentication of said first user based on said userID and password {Step 104 and Decision 105 of Figure 3A and Page 7 lines 1-4, and equivalents.}, and if said first user is authentic, forwarding to said application an authentication key for said first user and a selection by said first user pertaining to said application {Step 110 and Page 7 lines 9-13, and equivalents.}, said password not being sent from said protected network into said first network to access said application; and

said application including means for checking authentication of said key {Step 114 and 116 and Page 7 lines 13-14 or Page 7 line 23 to Page 8 line 1, and equivalents.}, and if authentic, complying with said selection by said first user {Step 124 and Page 8 lines 3-5, and equivalents.}; and

a workstation in a third, unprotected network {Red Zone 16 or Internet 54, and equivalents} for a second user {User 53 in Red Zone 16 or Internet 54, and equivalents}, said application being shared concurrently with said first and second users, said first network configured as a buffer between said second, protected network and said third, unprotected network; and wherein

said application receives from said second user another userID and another password, and includes means for determining that said other userID and other password are authentic {Step 306 and Decision 308, yes branch and Page 9 lines 1-5, and equivalents}, and in response, complying with a selection made by said second user pertaining to said application {Step 316 and Page 9 lines 3-5, and equivalents}.

Respectfully submitted,

Dated: 09/18/2007
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297